УДК 004.056

DOI 10.37468/2307-1400-2024-4-29-34

ЦИФРОВЫЕ ДВОЙНИКИ И БЕЗОПАСНОСТЬ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ: ПРАВОВЫЕ И ТЕХНОЛОГИЧЕСКИЕ АСПЕКТЫ

*Митяков Евгений Сергеевич*¹

¹ МИРЭА – Российский технологический университет, Москва, Россия

АННОТАЦИЯ

В условиях цифровизации критически важной инфраструктуры все большую значимость приобретают цифровые двойники – виртуальные модели физических объектов и процессов. Настоящая статья посвящена исследованию их потенциала в обеспечении информационной безопасности объектов критической информационной инфраструктуры (КИИ). В статье обсуждаются технологические возможности цифровых двойников (моделирование, прогнозирование и выявление угроз) и правовые аспекты их применения в рамках действующего законодательства РФ. Особое внимание уделено рискам, связанным с их интеграцией, включая нормативные пробелы, уязвимости систем и кадровые вызовы. В работе подчеркивается необходимость комплексного подхода к регулированию, разработке стандартов и подготовке специалистов для эффективного и безопасного внедрения цифровых двойников в КИИ.

Ключевые слова: цифровой двойник, критическая информационная инфраструктура, информационная безопасность, правовое регулирование, Индустрия 4.0, киберугрозы.

DIGITAL TWINS AND THE SECURITY OF CRITICAL INFORMATION INFRASTRUCTURE: LEGAL AND TECHNOLOGICAL ASPECTS

*Mityakov Evgeny S.*¹

¹ MIREA – Russian Technological University, Moscow, Russia

ABSTRACT

In the era of digitalization of critical infrastructure, digital twins – virtual models of physical objects and processes are gaining increasing importance. This article explores their potential in ensuring the cybersecurity of critical information infrastructure (CII). It addresses both the technological advantages of digital twins such as modeling, forecasting, and threat detection and the legal aspects of their application within the current legislation of the Russian Federation. Particular attention is given to the risks associated with their integration, including regulatory gaps, system vulnerabilities, and personnel challenges. The article emphasizes the need for a comprehensive approach to regulation, the development of standards, and the training of specialists to ensure the effective and secure implementation of digital twins in CII.

Keywords: digital twin, critical information infrastructure, cybersecurity, legal regulation, Industry 4.0, cyber threats.

Введение

Обеспечение информационной безопасности объектов критической информационной инфраструктуры (КИИ) – приоритетная задача в условиях цифровой трансформации. В соответствии со ст. 2 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – ФЗ-187), к объектам КИИ относятся информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления (АСУ), функционирующие в жизненно важных отраслях экономики и социальной сферы [1]. Нарушение безопасности таких объектов может повлечь серьезные последствия для жизненно важных отраслей. В этих условиях особую актуальность приобретает анализ новых технологических решений, активно внедряемых в КИИ. Одним из них выступают цифровые двойники (ЦД) – виртуальные копии физических объектов или процессов, которые стали неотъемлемой частью цифровизации промышленности, энергетики и транспорта. Однако их интеграция в КИИ требует строгого соблюдения законодательства в области информационной безопасности.

Цель настоящей работы заключается в анализе технологических и правовых аспектов использования ЦД в сфере КИИ.

Цифровые двойники: определение и роль в КИИ

В последние годы концепция ЦД находит применение в области обеспечения информационной безопасности. Например, в нефтегазовой отрасли ЦД используются для моделирования месторождений, что повышает эффективность добычи и предотвращает аварии [2].

Согласно ГОСТ Р 57700.37-2021, ЦД изделия определяется как «система, состоящая из цифровой модели изделия и двусторонних информационных связей с изделием (при наличии изделия) и (или) его составными частями» [3]. Это позволяет обеспечивать поддержку на всех стадиях жизненного цикла изделия – от разработки и производства до эксплуатации и модернизации. ЦД

в рамках объектов КИИ выступает виртуальной моделью информационных систем, ИТ-сетей или автоматизированных систем управления. Данная модель включает двустороннюю информационную связь с реальной системой, что дает возможность отслеживать ее состояние в реальном времени, моделировать угрозы, анализировать возможные последствия инцидентов и разрабатывать меры защиты.

В рамках Индустрии 4.0 ЦД становятся все более важным инструментом, превращаясь в универсальное средство для прогнозирования, анализа и оптимизации работы сложных систем. С точки зрения обеспечения информационной безопасности, они позволяют безопасно имитировать атаки, выявлять потенциальные уязвимости и оценивать риски без вмешательства в реальную инфраструктуру. Вместе с тем, их сочетание с такими передовыми технологиями, как киберфизические комплексы, промышленный интернет вещей и искусственный интеллект, не только открывает новые горизонты для управления инфраструктурой, но и создает дополнительные векторы для возможных кибератак [4, 5].

ЦД способен выявлять скрытые закономерности и неизвестные корреляции, что помогает в обнаружении новых угроз, ранее не идентифицированных традиционными методами. Возможности записи и мониторинга изменений системы позволяют проводить прогнозирование возможных инцидентов, тестировать различные сценарии защиты и оптимизировать решения для предотвращения угроз. Этот подход способствует снижению вероятности ошибок и повышению эффективности действий по защите КИИ [6].

С учетом возможностей ЦД для КИИ, в ряде исследований предпринимаются попытки формализации архитектуры систем управления информационной безопасностью с интеграцией компонентов ЦД [7, 8]. Важным условием является обеспечение взаимодействия ЦД с системами мониторинга, анализа инцидентов и автоматизированного принятия решений, которые должны опираться на актуальные и достоверные данные о состоянии объектов КИИ. Это позволит повы-

суть точность реагирования на угрозы, обеспечив своевременное принятие решений и эффективное управление в реальном времени [9].

Правовая основа регулирования цифровых двойников

ЦД, как модели, отражающие состояние и поведение физических объектов или процессов в реальном времени, подлежат отнесению к объектам КИИ в случаях, когда:

- они участвуют в управлении технологически значимыми объектами (например, электростанциями, узлами транспортной инфраструктуры);
- они обрабатывают информацию, связанную с обеспечением жизнедеятельности населения (например, модели распределения энергоресурсов в мегаполисах).

Субъекты КИИ обязаны обеспечивать защиту своих объектов. В частности, они должны:

- осуществлять категорирование объектов, определяя степень их значимости по утверждённым критериям: социальной, политической, экономической и экологической значимости, а также значимости для обороны и безопасности государства;
- использовать средства защиты информации, сертифицированные в соответствии с требованиями федеральных органов, включая ФСТЭК России.
- интегрировать свои системы с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА) и в случае инцидента – передавать информацию в установленном порядке.

Несоблюдение данных требований влечет административные штрафы и уголовную ответственность, если нарушения привели к тяжким последствиям (например, остановке производства из-за взлома ЦД) [10]. Таким образом, ЦД, вовлеченные в функционирование значимых объектов, подпадают под действие всех норм ФЗ-187, а субъекты, их эксплуатирующие, несут полную ответственность за соблюдение требований в области информационной безопасности.

Методические рекомендации ФСТЭК требуют оценивать объекты КИИ по критериям [11]:

- последствия нарушения работы (например,

сбой ЦД нефтепровода может вызвать остановку добычи);

- роль в критических процессах (если двойник участвует в управлении энергосетями или транспортом);
- интеграция с ГИС (цифровые модели, связанные с государственными системами, автоматически относятся к КИИ).

Например, ЦД атомной электростанции (АЭС), участвующий в управлении реактором и прогнозировании аварийных сценариев, подлежит категорированию как объект КИИ в силу его социальной и экологической значимости. Нарушение работы такой модели (например, внедрение вредоносного кода, способного исказить данные о температуре активной зоны), может привести к катастрофическим последствиям, которые повлекут за собой уголовную ответственность эксплуатанта объекта. Приведем еще один пример. Цифровая модель логистического узла морского порта, синхронизированная с государственной информационной системой (ГИС) мониторинга грузопотоков, автоматически относится к КИИ. Такая модель обрабатывает данные о перемещении опасных грузов (например, нефтепродуктов) и координирует работу крановых установок. Последствия ее компрометации включают экономические убытки (простой судов), экологический ущерб (разлив нефти) и угрозу жизни персонала. Субъект КИИ обязан оценить значимость ЦД по критерию «роль в критических процессах» и внедрить средства защиты, соответствующие требованиям ФЗ-187. Оба представленных примера показывают, как специфика функционирования ЦД и их интеграция с критически важными процессами формируют правовые и технические обязательства для субъектов КИИ.

Риски и вызовы интеграции цифровых двойников в КИИ

Внедрение ЦД в системы КИИ открывает новые возможности для оптимизации управления инфраструктурой, но сопряжено с комплексом рисков, требующих детального анализа. Эти риски охватывают технические, организационные и правовые аспекты, что делает их устранение много-

гранной задачей. Приведем их краткое описание.

1. Угрозы информационной безопасности. ЦД, непосредственно связанные с физическими объектами, выступают потенциальными точками входа для кибератак. Компрометация виртуальной модели может привести к деструктивным последствиям в реальном мире. Дополнительную сложность представляет уязвимость алгоритмов машинного обучения, применяемых в рамках ЦД.

2. Трудности категорирования. Отнесение ЦД к объектам КИИ различной категории значимости затрудняется их разнообразием, сложностью интеграции в бизнес-процессы и вариативностью последствий потенциального сбоя. Унифицированные методики оценки нередко оказываются недостаточными, что требует привлечения отраслевых экспертов и применения методов сценарного анализа.

3. Недостаточность нормативного регулирования. Существующая правовая база не в полной мере охватывает специфику функционирования ЦД. В частности, отсутствуют нормы, регулирующие такие характеристики, как динамическое обновление моделей, работа в распределенных средах, взаимодействие с облачными сервисами. Это создает неопределенность как в части правовой ответственности, так и в обеспечении прав субъектов данных. В данной связи актуальна разработка специализированных нормативных актов, регламентирующих эксплуатацию, аудит и безопасность ЦД.

4. Технические ограничения. Эффективность работы ЦД сопряжена с качеством исходных данных. Проблемы в каналах передачи информации, сбои в работе сенсоров или задержки в обновлении параметров могут вызвать искажения модели и привести к неверным решениям. В целях минимизации данных рисков целесообразна верификация данных в реальном времени, а также обеспечение резервирования критических компонентов ИКТ-инфраструктуры.

5. Организационные и кадровые вызовы. Успешное внедрение ЦД требует наличия высококвалифицированных специалистов, обладающих знаниями на пересечении информационных

технологий, операционных систем и информационной безопасности. На практике отмечается дефицит соответствующих кадров и сопротивление организационным изменениям со стороны персонала. Решением данной проблемы может стать развитие специализированных образовательных программ и междисциплинарных форматов подготовки специалистов.

6. Этические и социальные аспекты. Использование ЦД, особенно в отраслях, связанных с обработкой персональных данных (здравоохранение, транспорт), актуализирует вопросы конфиденциальности и прозрачности функционирования алгоритмов. Отсутствие ясности в принятии решений на основе моделей («эффект чёрного ящика») может снижать уровень доверия со стороны пользователей. Следовательно, необходима выработка этических стандартов, регулирующих порядок применения цифровых решений.

Заключение

ЦД становятся важным инструментом цифровизации КИИ, предоставляя новые возможности для моделирования, анализа и защиты сложных систем. Однако их внедрение связано с техническими, организационными, правовыми и этическими рисками. Отсутствие полноценного нормативного регулирования, сложности категорирования и зависимость от качества данных требуют комплексного подхода. Для эффективного и безопасного применения ЦД необходимо разработать стандарты, улучшить нормативно-правовую базу и подготовить квалифицированных специалистов.

Успешное внедрение этой технологии возможно только при междисциплинарном взаимодействии и системной подготовке кадров. Будущие исследования могут сосредоточиться на разработке архитектурных моделей ЦД для объектов КИИ и формализации критериев их категорирования и оценки рисков. Перспективным является создание интеллектуальных платформ, интегрирующих ЦД, искусственный интеллект и системы поддержки принятия решений в реальном времени. Особое внимание следует уделить

вопросам нормативной стандартизации, защиты персональных данных и этических аспектов в контексте эксплуатации цифровых моделей в чувствительных отраслях. Эти шаги помогут не только безопасной интеграции ЦД, но и укреплению национальной киберустойчивости.

Список литературы

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Федеральное агентство по правам на стандарты. – 2017. – URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 12.06.2023).
2. Как цифровые двойники помогают российской промышленности // Rusbase [Электронный ресурс]. – URL: <https://rb.ru/longread/digital-twin/> (дата обращения: 12.06.2023).
3. ГОСТ Р 57700.37-2021. Компьютерные модели и моделирование. Цифровые двойники изделий. Общие положения. – М.: Стандартинформ, 2022. – URL: <https://docs.cntd.ru/document/1200180928> (дата обращения: 12.06.2023).
4. Wang Y., Su Z., Guo S., Dai M., Luan T., Liu Y. A Survey on Digital Twins: Architecture, Enabling Technologies, Security and Privacy, and Future Prospects // IEEE Internet of Things Journal. – 2023. – V. 10. – P. 14965–14987. – DOI: 10.1109/JIOT.2023.3263909.
5. Masi M., Sellitto G., Aranha H., Pavleska T. Securing critical infrastructures with a cybersecurity digital twin // Software and Systems Modeling. – 2023. – V. 22. – P. 689–707. – DOI: 10.1007/s10270-022-01075-0.
6. Fei Tao, Bin Xiao, Qinglin Qi, Jiangfeng Cheng, Ping Ji. Digital twin modeling // Journal of Manufacturing Systems. – 2022. – V. 64. – P. 372–389. – ISSN: 0278-6125.
7. Попов А. М., Золотарев В. В., Кунц Е. Ю. Проблема управления информационной безопасностью при создании цифрового двойника дисциплины // Прикаспийский журнал: управление и высокие технологии. – 2022. – № 2 (58). – С. 109–118.
8. Касимова А. Р., Золотарев В. В., Сафиуллина Л. Х., Балыбердин А. С. Использование цифрового

двойника в задачах управления информационной безопасностью // Прикаспийский журнал: управление и высокие технологии. – 2023. – № 1 (61). – С. 48–58. – DOI 10.54398/20741707_2023_1_48. – EDN GVJYUN.

9. Isnaini K. N., Suhartono D. Evaluation of Basic Principles of Information Security at University Using COBIT 5 // MATRIK: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer. – 2022. – V. 21. – No 2. – P. 317–326.

10. Обзор изменений в законодательстве КИИ за май 2021 // Центр компетенций по вопросам обеспечения безопасности КИИ [Электронный ресурс]. – URL: <https://187.ussc.ru/news/detail/obzorzizm-may-2021/> (дата обращения: 12.06.2023).

11. Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» // ФСТЭК России [Электронный ресурс]. – URL: <https://fstec.ru/dokumenty/vse-dokumenty/postanovleniya/postanovlenie-pravitelstva-rossijskoj-federatsii-ot-8-fevralya-2018-g-n-127> (дата обращения: 12.06.2023).

References

1. Federal Law of July 26, 2017 No. 187-FZ “On the Security of Critical Information Infrastructure of the Russian Federation” // Federal Agency for Rights to Standards. - 2017. - URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (date of access: June 12, 2023).
2. How digital twins help Russian industry // Rusbase [Electronic resource]. - URL: <https://rb.ru/longread/digital-twin/> (date of access: June 12, 2023).
3. GOST R 57700.37-2021. Computer models and modeling. Digital twins of products. General provisions. – М.: Standartinform, 2022. – URL: <https://docs.cntd.ru/document/1200180928> (access date: 06/12/2023).
4. Wang Y., Su Z., Guo S., Dai M., Luan T., Liu Y. A Survey on Digital Twins: Architecture, Enabling

Technologies, Security and Privacy, and Future Prospects // IEEE Internet of Things Journal. – 2023. – V. 10. – P. 14965–14987. – DOI: 10.1109/JIOT.2023.3263909.

5. Masi M., Sellitto G., Aranha H., Pavleska T. Securing critical infrastructures with a cybersecurity digital twin // Software and Systems Modeling. – 2023. – V. 22. – P. 689–707. – DOI: 10.1007/s10270-022-01075-0.

6. Fei Tao, Bin Xiao, Qinglin Qi, Jiangfeng Cheng, Ping Ji. Digital twin modeling // Journal of Manufacturing Systems. – 2022. – V. 64. – P. 372–389. – ISSN: 0278-6125.

7. Popov A. M., Zolotarev V. V., Kunts E. Yu. The problem of information security management when creating a digital twin of a discipline // Caspian Journal: Management and High Technologies. – 2022. – No. 2 (58). – P. 109–118.

8. Kasimova A. R., Zolotarev V. V., Safiullina L. Kh., Balyberdin A. S. Using a digital twin in information security management tasks // Caspian Journal: Management and High Technologies. – 2023. – No. 1 (61). – P. 48–58. – DOI 10.54398/20741707_2023_1_48. – EDN GVJYUN.

9. Isnaini K. N., Suhartono D. Evaluation of Basic Principles of Information Security at University Using COBIT 5 // MATRIK: Jurnal Management, Information Technology and Computer Science. – 2022. – V. 21. – No. 2. – P. 317–326.

10. Review of changes in the critical information infrastructure legislation for May 2021 // Competence Center for Critical Information Infrastructure Security [Electronic resource]. – URL: <https://187.ussc.ru/news/detail/obzor-izm-may-2021/> (accessed: 12.06.2023).

11. Resolution of the Government of the Russian Federation of February 8, 2018 No. 127 “On approval of the Rules for categorizing critical information infrastructure facilities of the Russian Federation, as well as the list of indicators of significance criteria for critical information infrastructure facilities of the Russian Federation and their meanings” // FSTEC of Russia [Electronic resource]. – URL: <https://fstec.ru/dokumenty/vse-dokumenty/postanovleniya/postanovlenie-pravitelstva-rossijskoj-federatsii-ot-8-fevralya-2018-g-n-127> (date of access: 12.06.2023).

*Статья поступила в редакцию 14 августа 2024 г.
Принята к публикации 23 декабря 2024 г.*

Ссылка для цитирования: Митяков Е.С. Цифровые двойники и безопасность критической информационной инфраструктуры: правовые и технологические аспекты // Национальная безопасность и стратегическое планирование. 2024. № 4(48). С. 29–34. DOI: <https://doi.org/10.37468/2307-1400-2024-4-29-34>

For citation: Mityakov E.S. Digital twins and the security of critical information infrastructure: legal and technological aspects // National security and strategic planning. 2024. № 4(48). pp. 29–34. DOI: <https://doi.org/10.37468/2307-1400-2024-4-29-34>

Сведения об авторах:

МИТЯКОВ ЕВГЕНИЙ СЕРГЕЕВИЧ – доктор экономических наук, профессор, профессор кафедры информатики, Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА – Российский технологический университет», г. Москва, Россия

ORCID: <https://orcid.org/0000-0001-6579-0988>

SPIN-код: 5691-8947

e-mail: iyao@mail.ru

Information about authors:

MITYAKOV EVGENII S. – Doctor of Economics, Professor, Professor the Computer Science Department, Federal State Budgetary Educational Institution of Higher Education “MIREA – Russian Technological University”, Moscow, Russia

ORCID: <https://orcid.org/0000-0001-6579-0988>

SPIN: 5691-8947

e-mail: iyao@mail.ru